Dstny – Senior Operations Security Engineer

The Senior Operations Security Engineer is responsible for securing the Product & Technology Organisation's platforms, infrastructure and cloud services. This includes the products that run on the platform — Dstny Voice, Dstny Digital Agents, Dstny Call2Teams and Dstny Intelligence — as well as legacy products that remain in production. This role reports to the VP Platform Operations.

Working within the Operations team, this is a hands-on role focused on implementing security controls, reducing operational risk, improving platform resilience and strengthening security capabilities across production environments.

You will work closely with Platform Engineering, Development and Architecture teams to ensure security is embedded into both day-to-day operations and future platform designs.

Security Engineering & Operations

- Design, implement and operate security controls across cloud platforms, infrastructure and production services.
- Improve monitoring, detection, alerting and incident response capabilities.
- Lead technical investigation and remediation of security incidents.
- Manage vulnerability remediation and drive risk reduction activities.
- Automate security controls, processes and reporting.
- Perform threat hunting and continuously improve security visibility.
- Secure the products delivered on the platform (Dstny Voice, Digital Agents, Call2Teams and Intelligence), including AI and digital agent services and real-time communications threats such as telecom fraud and SIP abuse.

Cloud & Platform Security

- Secure Azure/AWS environments, Kubernetes platforms and cloud-native services.
- Harden operating systems, containers and production environments.
- Improve identity, access and privileged account management.
- Review infrastructure, platform and API designs to identify and mitigate security risks.
- Support disaster recovery, resilience testing and operational risk reduction.
- Maintain tenant isolation and service-provider channel security across the shared, multi-tenant platform, including legacy products still in production.

Collaboration

- Work closely with Platform Engineering, Development and Architecture teams to embed security into technical solutions.
- Work with the Data Protection Officer (DPO) and the Compliance team on privacy and regulatory requirements.

- Provide practical security guidance during projects and major platform changes.
- Support compliance activities including ISO 27001, NIS2, GDPR and customer security requirements.
- Contribute to security standards, best practices and continuous improvement initiatives.

Required Experience

- Security engineering, security operations and incident response.
- Vulnerability management and threat detection.
- Linux administration and networking fundamentals.
- Azure and/or AWS.
- Kubernetes and container technologies.
- Infrastructure-as-Code (Terraform or similar).
- Scripting and automation (PowerShell, Python, Bash or Go).
- CI/CD, Git and modern operational practices.
- Security monitoring, SIEM and observability platforms.

Nice to Have

- Experience in SaaS, UCaaS or telecommunications environments.
- Experience securing large-scale customer-facing platforms.
- Knowledge of Microsoft Defender, Sentinel, Wiz, Prisma Cloud or similar tools.
- Experience with SOAR and security automation.
- Relevant security certifications.

What Success Looks Like

- Improved security posture across PTO platforms and services.
- Reduced vulnerability exposure and operational risk.
- Increased maturity of monitoring, detection and incident response.
- Improved resilience of cloud and production platforms.
- Security controls that scale with business growth.
- Trusted security partnership across Operations, Engineering and Product teams.

https://dstny.com/